What is claimed is:

1. A method for authenticating one or more instantiations of a product following initial distribution comprising:

providing a code string model having finite parameters, the finite parameters used to define a total quantity of unique code strings that can be derived from the code string model;

providing a subset of unique code strings as a quantity of unique code strings selected for use from the total quantity of unique code strings, the subset of unique code strings being at least one hundred times smaller than the total quantity of unique code strings;

defining a maximum probability of guessing any of the subset of unique code strings;

verifying that an actual probability of guessing any of the subset of unique code strings is less than the maximum probability of guessing any of the subset of unique code strings;

randomly generating the subset of unique code strings from the total quantity of unique code strings;

providing a secure server having a database used to store the subset of unique code strings;

storing the subset of unique code strings within the database on the secure server;

marking each of a quantity of the instantiations with one of the code strings of the subset;

distributing the marked instantiations along a chain of commerce; and

validating the authenticity of one of the marked instantiations during or following distribution, the marked instantiation validated through exchange of transmitted signals between the secure server and a communication device, the communication device adapted for entry of the unique code string and adapted to transmit an inquiry signal containing the unique code string to the secure server, the secure server adapted to receive the inquiry signal to reveal the scanned unique code string, adapted to search the database thereon to

validate the authenticity of the unique code string, and adapted to transmit a return signal to the field reader regarding validation of the authenticity of the marked instantiation.

2. The method of claim 1, wherein the code string model providing step further includes defining the finite parameters as code string length and code string character types.

3. The method of claim 1, wherein the code string model providing step further includes defining the code string model to be a serial number, whereby the finite parameters include having at least seven characters and having each of the characters be defined alphanumerically.

4. The method of claim 1, wherein the probability verifying step further includes defining the maximum probability to be one in eighty million.

5. The method of claim 1, wherein the probability verifying step further includes providing one of (a) a new code string model having a larger string length and (b) a greater quantity of code string character types, provided that the actual probability of guessing any of the subset of unique code strings is greater than the maximum probability of guessing any of the subset of unique code strings.

6. The method of claim 1, wherein the subset of unique code strings storing step further includes only storing the unique code strings of the subset that are marked on the instantiations.

7. The method of claim 1, wherein the marking instantiations step further includes providing products from one of a plurality of technologies involving electronics, branded product enhancers, aerospace, automotive, and pharmaceutical.

8. The method of claim 1, wherein the marking instantiations step comprises marking each unique code string of the subset on a corresponding tag.

9. The method of claim 8, wherein the marking instantiations step comprises affixing the marked tags to corresponding instantiations.

10. The method of claim 1, wherein the marking instantiations step comprises using the process of microprinting.

11. The method of claim 10, wherein variable microprinting is used so that one or more portions of the unique code strings of the subset are each designated with a color, and wherein the unique code strings of the subset have a color pattern.

12. The method of claim 11, wherein the color pattern of each unique code string of the subset is comprised of a plurality of colors, and wherein the color pattern is varied in an orderly fashion among the unique code strings of the subset so as to provide a set of alternating color patterns among the unique code strings of the subset.

13. The method of claim 1, wherein the authenticity validation step further includes manually keying the unique code string into a keypad of the communication device.

14. The method of claim 1, wherein the authenticity validation step further includes providing a cellular phone as the communication device.

15. The method of claim 1, wherein the authenticity validation step further includes using the Internet as a network for transmitting and receiving the inquiry and return signals.

16. The method of claim 1, wherein the secure server providing step further includes attaching the server to an Internet website.

17. The method of claim 16, wherein the secure server providing step further includes providing an intermediary Internet website adapted to automatically shift the inquiry signals from the communication device to one of a plurality of Internet websites providing the secure server and database, wherein the one of the plurality of websites corresponds to the manufacturer of the product to be authenticated.

18. The method of claim 1, wherein the authenticity validation step further includes using a check-sum algorithm before validation to initially authenticate the unique code strings without having to search the database.

19. The method of claim 1, wherein the authenticity validation step further includes using an algorithm before validation to initially obtain approval in accessing the secure server.

20. The method of claim 19, wherein the algorithm is used to identify embedded IP addresses within the unique code strings of the subset, wherein the identified IP addresses are understood as being solely acceptable with respect to inquiries made to the secure server.

21. A method for authenticating and tracking one or more instantiations of a product following initial distribution comprising:

providing a code string model having finite parameters, the finite parameters used to define a total quantity of unique code strings that can be derived from the code string model;

providing a subset of unique code strings as a quantity of unique code strings selected for use from the total quantity of unique code strings, the subset of unique code strings being at least one hundred times smaller than the total quantity of unique code strings;

defining a maximum probability of guessing any of the subset of unique code strings;

verifying that an actual probability of guessing any of the subset of unique code strings is less than the maximum probability of guessing any of the subset of unique code strings;

randomly generating the subset of unique code strings from the total quantity of unique code strings;

associating attributes to one or more of the subset of unique code strings, the attributes defining characteristics regarding the instantiations to which the one or more of the subset of unique code strings will be marked on or affixed to;

providing a secure server having a database used to store the subset of unique code strings;

storing the subset of unique code strings within the database on the secure server;

marking each of a quantity of the instantiations with one of the code strings of the subset;

distributing the marked instantiations along a chain of commerce; and

validating the authenticity of one of the marked instantiations during distribution, the marked instantiation validated through exchange of transmitted signals between the secure server and a communication device, the communication device adapted for entry of the unique code string and adapted to transmit an inquiry signal containing the unique code string to the secure server, the secure server adapted to receive the inquiry signal to reveal the scanned unique code string, adapted to search the database thereon to validate the authenticity of the unique code string, and adapted to transmit a return signal to the field reader regarding validation of the authenticity of the marked instantiation.

22. The method of claim 21, wherein the storing step further includes storing the attributes assigned to the unique code strings within the database of the secure server.

23. The method of claim 22, wherein the validating authenticity step further includes searching the database for the attributes in order to determine tracking parameters of the marked instantiations.

24. The method of claim 22, wherein the validating authenticity step further includes storing current location information of the marked instantiations if the tracking parameters are determined to be valid.

25. The method of claim 21, wherein the marking instantiations step comprises marking each unique code string of the subset on a corresponding label.

26. The method of claim 25, wherein the marking instantiations step comprises affixing the marked labels to corresponding instantiations.

27. The method of claim 21, wherein the marking instantiations step comprises using the process of watermarking.

28. The method of claim 27, wherein the watermarking process comprises digital watermarking, and wherein the unique code strings of the subset are each embedded in a corresponding label.

29. The method of claim 28, wherein a deciphering step is performed to identify each of the embedded unique code strings of the subset before the unique codes strings of the subset can be authenticated.

30. The method of claim 21, wherein the authenticity validation step further includes using a schema for the exchange of transmitted signals between the secure server and the communication device, and wherein the schema is an industry standard.

31. The method of claim 30, wherein the schema is of an XML format.

32. A method for authenticating one or more instantiations of a product following initial distribution comprising:

providing a code string model having finite parameters, the finite parameters used to define a total quantity of unique code strings that can be derived from the code string model;

providing a subset of unique code strings as a quantity of unique code strings selected for use from the total quantity of unique code strings, the subset of unique code strings being at least one hundred times smaller than the total quantity of unique code strings;

defining a maximum probability of guessing any of the subset of unique code strings;

verifying that an actual probability of guessing any of the subset of unique code strings is less than the maximum probability of guessing any of the subset of unique code strings;

randomly generating the subset of unique code strings from the total quantity of unique code strings;

providing a secure server having a database used to store the subset of unique code strings, the secure server;

storing the subset of unique code strings within the database on the secure server;

marking each of a quantity of the instantiations with one of the code strings of the subset;

distributing the marked instantiations along a chain of commerce; and

validating the authenticity of one of the marked instantiations during distribution, the marked instantiation validated through exchange of transmitted signals between the secure server and a field reader, the field reader adapted to scan the unique code string on the marked instantiation, adapted to encode the unique code string into a machine-readable format, and adapted to transmit an inquiry signal containing the encoded unique code string to the secure server, the secure server adapted to decode the inquiry signal to reveal the scanned unique code string, adapted to search the database thereon

to validate the authenticity of the unique code string, and adapted to transmit a return signal to the field reader regarding validation of the authenticity of the marked instantiation.

33. The method of claim 32, wherein the authenticity validation step further includes providing a laser scanner as the field reader.

34. The method of claim 32, wherein the authenticity validation step further includes logging the validation and storing this logging information.

35. The method of claim 34, wherein the logged information is checked against future authenticity validations to aid in their invalidation based on implausible location changes of the unique code strings of the subset.

36. The method of claim 35, wherein the location changes are identified through the corresponding IP addresses and compared against time lapse between subsequent authenticity validations.

37. A system for authenticating one or more instantiations of a product following initial distribution comprising:

a subset of a total quantity of unique code strings derived from a code string model, the code string model having finite parameters of code string length and code string character types, the finite parameters defining the total quantity of unique code strings, the subset of unique code strings being at least one hundred times smaller than the total quantity of unique code strings, each of the subset of unique code strings marked on one of the instantiations;

a secure server having a database adapted for storing the subset of codes therein;

a communication device adapted for entry therein of one of the subset of unique code strings and adapted to transmit an inquiry signal containing the unique code string to the secure server, the secure

server adapted for receiving the inquiry signal, adapted to search the database thereon to validate the authenticity of the unique code string, and adapted to transmit a return signal to the communication device regarding validation of the authenticity of the marked instantiations; and

a network linking the secure server to the communication device, the network comprising the Internet.

38. The system of claim 37, wherein the code string model comprises a serial number, wherein the finite parameters include having at least seven characters and having each of the characters be defined alphanumerically.

39. The system of claim 37, wherein the communication device includes a keypad used for manual entry of the unique code string.

40. The method of claim 37, wherein the communication device comprises a cellular phone.

41. The system of claim 37, wherein the Internet includes a website attaching the secure server thereto.

42. The system of claim 37, wherein the Internet includes an intermediary website adapted to automatically shift the incoming signals from the communication device to one of a plurality of websites to which the secure server is attached, the one of the plurality of websites corresponding to a manufacturer of the marked instantiation.

43. The system of claim 37, wherein the Internet includes a plurality of websites each having access to the stored unique code strings via one or more of the secure server and other secure servers.

44. The system of claim 43, wherein the plurality of websites is each adapted to provide authenticity validation with respect to a set of the one or more instantiations of the product that are marked with the unique code strings of the subset.

45. The system of claim 44, wherein each set designates a quantity of the one or more instantiations of the product that is at most equal to the quantity of the unique code strings in the subset.

46. A system for authenticating one or more instantiations of a product following initial distribution comprising:

a subset of a total quantity of unique code strings derived from a code string model, the code string model having finite parameters of code string length and code string character types, the finite parameters defining the total quantity of unique code strings, the subset of unique code strings being at least one hundred times smaller than the total quantity of unique code strings, each of the subset of unique code strings marked on one of the instantiations;

a secure server having a database adapted for storing the subset of codes therein;

a field reader adapted to scan one of the subset of unique code strings, adapted to encode the unique code string into a machine-readable format, and adapted to transmit an inquiry signal containing the encoded unique code string to the secure server, the secure server adapted for decoding the inquiry signals, adapted to search the database thereon to validate the authenticity of the unique code string, and adapted to transmit a return signal to the field reader regarding validation of the authenticity of the marked instantiations; and

a network linking the secure server to the field reader.

47. The system of claim 46, wherein the field reader comprises a laser scanner.

48. The system of claim 46, wherein the unique code strings have certain expiration dates associated therewith.

49. The system of claim 48, wherein each of the unique code strings having certain expiration dates is adapted to expire by being deleted from the secure server on the corresponding expiration date.